ABSTRACT

Wireless Sensor Network is a network system comprised of spatially distributed devices using wireless sensor nodes to monitor physical or environmental conditions, such as sound, temperature and motion. The individual nodes are capable of sensing their environments, processing the information data locally and sending data to one or more collection points in a WSN.

Clustering methods are more advantageous than the flat routing in the WSNs. They are categorized into member nodes and group/cluster heads. The group/cluster heads are more vulnerable to attacks since they hold responsible positions inside the WSN. In an effort to solve this problem, this research work focuses on the trust management methods for hierarchical WSNs to increase the security.

Four novel methods aiming at solving internal attacks and providing trust in hierarchical WSN are proposed. They are: Enhance Node-based Trust Management; Trust based Energy Efficient scheme for Hierarchical Clustering; Hierarchical Trust Based Efficient Cluster Head Selection in WSN; and Efficient Data Collection based on Trust Evaluation for WSNs.

Firstly, an Enhanced Node-based Trust Management (ENTM) scheme is proposed based on a Clustered mobile sensor network with backbone. It introduces the trust of a node within local management strategy with the help from the mobile agents running on each node. When the participating nodes have discovered their neighbors, they exchange information about the number of one hop neighbors. The

nodes update the trust values and the clusters are formed in the network Algorithm. This protocol thereby increases the secure communication in a hierarchical WSN.

Secondly, Trust based Energy Efficient scheme for Hierarchical Clustering (TEEHC) aims to minimize the energy cost and maximize the security in WSN. All sensor nodes are stationary and clusters of sensors can be formed based on the location. A CH is in charge of its cluster and receives the information from different sensors, processes the data to extract relevant information and then sends it to the BS via multi-hop transmission.

The third method, Hierarchical Trust based Efficient Cluster Head selection in WSN (HTECH) demonstrates the CH selection process based on Trust based routing in WSN. The trust evaluation is based on the SN cooperativeness, SN Unselfishness, SN honest and SN data transmission rate. This trusted route provides a realistic and secure approach to choose a shortest path in all trusted path by using hierarchical trust phase and efficient CH selection phase.

Finally, Efficient Data Collection based on Trust Evaluation (EDCTE) is proposed to improve the reliability of data aggregation and energy efficiency. The EDCTE scheme consists of set-up phase and steady state phase. It can be used to detect the malevolent node to provide the trust relationship between nodes.

A comparative analysis of the four protocols ENTM, TEEHC, HTECH and EDCTE is performed. All simulations are achieved in the network simulator tool that uses various scenarios (50 nodes and 100 nodes) for comparison against baseline protocols. There is a lot of scope for research with the increasing usage of the WSNs and in future real world scenarios are also suggested for implementation.